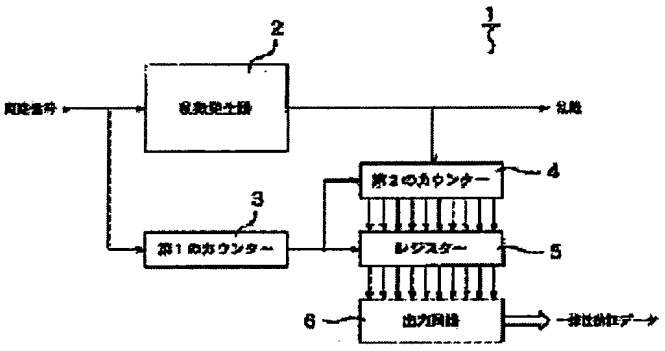
1-BIT RANDOM NUMBER GENERATOR, MULTI-BIT RANDOM NUMBER GENERATOR ANI PROBABILITY GENERATOR

Patent number:	JP2003029963
Publication date:	2003-01-31
Inventor:	YAMAMOTO HIROYASU; SHIGA TAKAAKI; SHIMIZU TAKAKUNI; KOIBUCHI MISAKO
Applicant:	FDK CORP
Classification:	
- international:	G06F7/58; G09C1/00
- european:	
Application number:	JP20010216704 20010717
Priority number(s):	JP20010216704 20010717

Abstract of **JP2003029963**

PROBLEM TO BE SOLVED: To easily verify the appearance uniformity of random number data and to improve reliability in a random number generator and a probability generator utilized in scientific and technical calculations or the like. SOLUTION: The random number generator 2 outputting '1' and '0' as the random number data is provided with a first counter 3 counting the fixed number of times and a second counter 4 counting the number of times of the appearance of the random number data and generating the number-of-times data. A register 5 holds the number-of-times data of the second counter 4 for each cycle counted in the first counter 3 and an output circuit 6 outputs the number-of-times data held in the register 5 as verification data. Thus, the appearance uniformity of the random number data can be verified by itself and the need that a user perform a statistic processing is eliminated.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－29963
（P2003－29963A）
(43)公開日　平成15年１月31日(2003.1.31)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　7/58		Ｃ０６Ｆ　7/58	Ａ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６５０	Ｃ０９Ｃ　1/00	６５０Ｂ	

審査請求　有　　請求項の数11　ＯＬ　（全 16 頁）

(21)出願番号　特願2001－216704(P2001－216704)

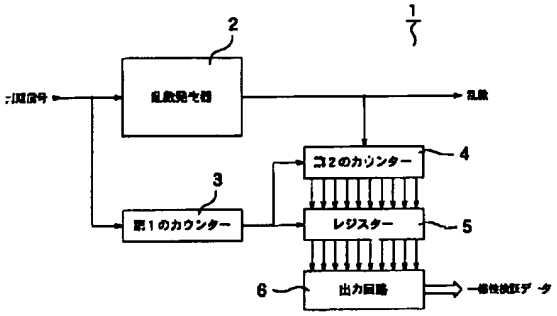
(22)出願日　平成13年７月17日(2001.7.17)

(71)出願人　00023/721
エフ・ディ・・ケイ株式会社
東京都港区新橋５丁目36番11号
(72)発明者　山本　博康
東京都港区新橋５丁目36番11号　いわき電子株式会社内
(72)発明者　志賀　隆則
東京都港区新橋５丁目36番11号　いわき電子株式会社内
(74)代理人　10006/046
弁理士　尾股　行雄　（外１名）

最終頁に続く

(54)【発明の名称】　１ビット乱数発生装置および多数ビット乱数発生装置ならびに確率発生装置

(57)【要約】
【課題】　科学技術計算などに利用される乱数発生装置および確率発生装置において、乱数データの出現一様性を手軽に検証して信頼性を高める。
【解決手段】　乱数データとして「１」と「０」を出力する乱数発生器２に、一定回数を計数する第１のカウンター３と、乱数データの出現回数を計数して回数データを生成する第２のカウンター４とを備える。第１のカウンター３で計数された周期ごとに第２のカウンター４の回数データをレジスター５が保持し、レジスター５に保持された回数データを出力回路６が検証データとして出力する。これにより、乱数データの出現一様性を自ら検証でき、使用者が統計処理を行う必要がなくなる。



【特許請求の範囲】
【請求項1】 乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、
一定回数を計数する第1のカウンター(3)と、前記乱数発生器から出力された乱数データの出現回数を計数して回数データを生成する第2のカウンター(4)とを備え、
第1のカウンターで計数された周期ごとに第2のカウンターの回数データを保持するレジスター(5)を備え、
このレジスターに保持された回数データを検証データとして出力する出力回路(6)を備えたことを特徴とする1ビット乱数発生装置。
【請求項2】 出力回路(6)に代えて、
予め設定された上限比較データおよび下限比較データとレジスター(5)に保持されたデータとを比較して検証信号を出力する比較器(7)を備えたことを特徴とする請求項1に記載の1ビット乱数発生装置。
【請求項3】 乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、
この乱数発生器から出力された前回の乱数データを保持するデータ保持器(8)を備え、
前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器(9)を備え、
前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアするカウンター(10)を備え、
このカウンターに保持されたデータを検証データとして出力する出力回路(6)を備えたことを特徴とする1ビット乱数発生装置。
【請求項4】 乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、
この乱数発生器から出力された前回の乱数データを保持するデータ保持器(8)を備え、
前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する第1の比較器(11)を備え、
第1の比較器からカウントアップ信号を受けたときにカウントアップするとともに、第1の比較器からカウントクリア信号を受けたときにカウントクリアするカウンター(10)を備え、
このカウンターの出力データを保持するレジスター(12)を備え、
このレジスターのデータと前記カウンターの出力データとを比較して、前者より後者の方が大きいときにデータ上書き信号を出力するとともに、それ以外のときにデータ保持信号を出力する第2の比較器(13)を備え、
第2の比較器からデータ上書き信号を受けたときに前記カウンターの出力データを前記レジスターに書き込むとともに、第2の比較器からデータ保持信号を受けたときに前記レジスターのデータを保持するように制御する制御回路(14)を備え、
前記レジスターに保持されたデータを検証データとして出力する出力回路(15)を備えたことを特徴とする1ビット乱数発生装置。
【請求項5】 出力回路(15)に代えて、
予め設定された比較データとレジスター(12)に保持されたデータとを比較して検証信号を出力する第3の比較器(16)を備えたことを特徴とする請求項4に記載の1ビット乱数発生装置。
【請求項6】 乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、
一定回数を計数する第1のカウンター(17)を備え、
前記乱数発生器から出力された前回の乱数データを保持するデータ保持器(8)を備え、
前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器(9)を備え、
前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアする第2のカウンター(18)を備え、
第2のカウンターの出力データをデコードして各信号長ごとに出力するデコーダー(19)を備え、
このデコーダーの出力データを各信号長ごとにそれぞれカウントする複数個の第3のカウンター(20)を備え、
第1のカウンターで計数された一定回数ごとに第3の各カウンターの出力データをそれぞれ保持する複数個のレジスター(21)を備え、
第1のカウンターで計数された一定回数ごとの信号と前記比較器の出力データとに基づいて前記各レジスターから検証データを出力するように制御する制御回路(22)を備えたことを特徴とする1ビット乱数発生装置。
【請求項7】 レジスター(21)の出力データを選択して出力する選択回路(23)を付設したことを特徴とする請求項6に記載の1ビット乱数発生装置。
【請求項8】 請求項1または請求項3または請求項4または請求項6または請求項7に記載の1ビット乱数発生装置(1)を複数個並列に接続し、
これら1ビット乱数発生装置から出力された検証データをビットごとに選択して出力する選択回路(26)を付設したことを特徴とする多数ビット乱数発生装置。

【請求項9】　請求項2または請求項5に記載の1ビット乱数発生装置（24）を複数個並列に接続し、
これら1ビット乱数発生装置から出力された検証信号をビットごとに選択して出力する選択回路（27）を付設したことを特徴とする多数ビット乱数発生装置。
【請求項10】　請求項1から請求項7までのいずれかに記載の1ビット乱数発生装置（1、24）を有し、
この1ビット乱数発生装置から出力された乱数データをシリアルデータからパラレルデータへ変換するシフトレジスター（31）を備え、
一定のパラレルデータのビット長を計数するカウンター（32）を備え、
このカウンターで計数された周期ごとに前記シフトレジスターのパラレルデータを保持するレジスター（33）を備え、
予め設定された確率上限データおよび確率下限データと前記レジスターに保持されたパラレルデータとを比較して確率信号を出力する比較器（34）を備えたことを特徴とする確率発生装置。
【請求項11】　請求項8または請求項9に記載の多数ビット乱数発生装置（25）を有し、
予め設定された確率上限データおよび確率下限データと前記多数ビット乱数発生装置から出力された乱数データとを比較して確率信号を出力する比較器（35）を備えたことを特徴とする確率発生装置。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、科学技術計算、ゲーム機、或いは暗号化処理などに利用するに好適な1ビット乱数発生装置および多数ビット乱数発生装置と、これらを用いた確率発生装置に関するものである。
【0002】
【従来の技術】一般に、乱数発生器を備えた乱数発生装置（1ビット乱数発生装置、多数ビット乱数発生装置）や確率発生装置において、その製品としての信頼性を高めるためには、乱数発生器から送出される乱数データに前後関係、規則性、周期性がないことに加えて、この乱数データに出現一様性（乱数によって出現率に差異が生じないこと）があることが重要となる。そのため従来は、乱数発生器から連続的に送出された膨大の乱数データを使用者が統計処理してその出現一様性を検証していた。
【0003】
【発明が解決しようとする課題】しかし、これでは乱数データの統計処理が面倒で煩雑となるので、出現一様性の検証に手間がかかるという不都合があった。
【0004】本発明は、このような事情に鑑み、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な1ビット乱数発生装置および多数ビット乱数発生装置ならびに確率発生装置を提供することを目的とする。
【0005】
【課題を解決するための手段】本発明では、1ビット乱数発生装置および多数ビット乱数発生装置ならびに確率発生装置の製品としての信頼性を高めるべく、乱数データの出現一様性を自ら検証できる機能を内蔵することに着目した。
【0006】すなわち、本発明のうち請求項1に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、一定回数を計数する第1のカウンター（3）と、前記乱数発生器から出力された乱数データの出現回数を計数して回数データを生成する第2のカウンター（4）とを備え、第1のカウンターで計数された周期ごとに第2のカウンターの回数データを保持するレジスター（5）を備え、このレジスターに保持された回数データを検証データとして出力する出力回路（6）を備えて構成される。
【0007】また、本発明のうち請求項2に係る発明は、上記出力回路（6）に代えて、予め設定された上限比較データおよび下限比較データと上記レジスター（5）に保持されたデータとを比較して検証信号を出力する比較器（7）を備えて構成される。
【0008】また、本発明のうち請求項3に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、この乱数発生器から出力された前回の乱数データを保持するデータ保持器（8）を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器（9）を備え、前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアするカウンター（10）を備え、このカウンターに保持されたデータを検証データとして出力する出力回路（6）を備えて構成される。
【0009】また、本発明のうち請求項4に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、この乱数発生器から出力された前回の乱数データを保持するデータ保持器（8）を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する第1の比較器（11）を備え、第1の比較器からカウントアップ信号を受けたときにカウントアップするとともに、第1の比較器からカウントクリア信号を受けたときにカウントクリアするカウンター（10）を備え、このカウンターの出力データを保持するレジスター（12）を備え、このレジスターのデータと前記カウン

ターの出力データとを比較して、前者より後者の方が大きいときにデータ上書き信号を出力するとともに、それ以外のときにデータ保持信号を出力する第2の比較器（13）を備え、第2の比較器からデータ上書き信号を受けたときに前記カウンターの出力データを前記レジスターに書き込むとともに、第2の比較器からデータ保持信号を受けたときに前記レジスターのデータを保持するように制御する制御回路（14）を備え、前記レジスターに保持されたデータを検証データとして出力する出力回路（15）を備えて構成される。

【0010】また、本発明のうち請求項5に係る発明は、上記出力回路（15）に代えて、予め設定された比較データと上記レジスター（12）に保持されたデータとを比較して検証信号を出力する第3の比較器（16）を備えて構成される。

【0011】また、本発明のうち請求項6に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器（2）を有し、一定回数を計数する第1のカウンター（17）を備え、前記乱数発生器から出力された前回の乱数データを保持するデータ保持器（8）を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器（9）を備え、前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアする第2のカウンター（18）を備え、第2のカウンターの出力データをデコードして各信号長ごとに出力するデコーダー（19）を備え、このデコーダーの出力データを各信号長ごとにそれぞれカウントする複数個の第3のカウンター（20）を備え、第1のカウンターで計数された一定回数ごとに第3の各カウンターの出力データをそれぞれ保持する複数個のレジスター（21）を備え、第1のカウンターで計数された一定回数ごとの信号と前記比較器の出力データとに基づいて前記各レジスターから検証データを出力するように制御する制御回路（22）を備えて構成される。

【0012】また、本発明のうち請求項7に係る発明は、上記レジスター（21）の出力データを選択して出力する選択回路（23）を付設して構成される。

【0013】また、本発明のうち請求項8に係る発明は、上記1ビット乱数発生装置（1）を複数個並列に接続し、これら1ビット乱数発生装置から出力された検証データをビットごとに選択して出力する選択回路（26）を付設して構成される。

【0014】また、本発明のうち請求項9に係る発明は、上記1ビット乱数発生装置（24）を複数個並列に接続し、これら1ビット乱数発生装置から出力された検証信号をビットごとに選択して出力する選択回路（27）を付設して構成される。

【0015】また、本発明のうち請求項10に係る発明は、上記1ビット乱数発生装置（1、24）を有し、この1ビット乱数発生装置から出力された乱数データをシリアルデータからパラレルデータへ変換するシフトレジスター（31）を備え、一定のパラレルデータのビット長を計数するカウンター（32）を備え、このカウンターで計数された周期ごとに前記シフトレジスターのパラレルデータを保持するレジスター（33）を備え、予め設定された確率上限データおよび確率下限データと前記レジスターに保持されたパラレルデータとを比較して確率信号を出力する比較器（34）を備えて構成される。

【0016】さらに、本発明のうち請求項11に係る発明は、上記多数ビット乱数発生装置（25）を有し、予め設定された確率上限データおよび確率下限データと前記多数ビット乱数発生装置から出力された乱数データとを比較して確率信号を出力する比較器（35）を備えて構成される。

【0017】これらの構成において、データ保持器の代表例としてDタイプフリップフロップを挙げることができ、比較器の代表例としては排他的論理和素子（EXCLUSIVE-OR素子）を挙げることができる。そして、こうした構成を採用することにより、乱数データの出現一様性を自ら検証することが可能となり、使用者が統計処理を行う必要がなくなるように作用する。

【0018】なお、括弧内の符号は図面において対応する要素を表す便宜的なものであり、したがって、本発明は図面上の記載に限定拘束されるものではない。このことは「特許請求の範囲」の欄についても同様である。

【0019】

【発明の実施の形態】以下、本発明の実施形態を図面に基づいて説明する。

【0020】図1は本発明に係る1ビット乱数発生装置の第1の実施形態を示す回路図である。

【0021】この1ビット乱数発生装置1は、図1に示すように、乱数発生器2、第1のカウンター3、第2のカウンター4、レジスター5および出力回路6から構成された検証データ出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、乱数発生器2の入力信号が第1のカウンター3にも入力され、第1のカウンター3は一定回数を計数して第2のカウンター4およびレジスター5に出力する。一方、第2のカウンター4は、乱数発生器2から出力された乱数データの出現回数を計数して回数データを生成する。そして、レジスター5は、第1のカウンター3で計数された周期ごとに第2のカウンター4の回数データを保持し、出力回路6は、レジスター5に保持された回数データを検証データとしてシリアルまたはパラレルに出力する。

【0022】したがって、この1ビット乱数発生装置1

では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

【００２３】図２は本発明に係る１ビット乱数発生装置の第２の実施形態を示す回路図である。

【００２４】この１ビット乱数発生装置２４は、図２に示すように、乱数発生器２、第１のカウンター３、第２のカウンター４、レジスター５および比較器７から構成された検証信号出力型であり、乱数発生器２に同期信号が入力されると、乱数発生器２から乱数データとして「１」または「０」が出力される。このとき、乱数発生器２の入力信号が第１のカウンター３にも入力され、第１のカウンター３は一定回数を計数する。一方、第２のカウンター４は、乱数発生器２から出力された乱数データの出現回数を計数して回数データを生成する。そして、レジスター５は、第１のカウンター３で計数された周期ごとに第２のカウンター４の回数データを保持する。さらに、比較器７は、レジスター５に保持されたデータと予め設定された上限比較データおよび下限比較データとを比較し、レジスター５内のデータが上限比較データと下限比較データとの間にある場合には乱数データの出現一様性が高い旨の検証信号を出力し、それ以外の場合には乱数データの出現一様性が低い旨の検証信号を出力する。

【００２５】したがって、この１ビット乱数発生装置２４では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

【００２６】図３は本発明に係る１ビット乱数発生装置の第３の実施形態を示す回路図である。

【００２７】この１ビット乱数発生装置１は、乱数発生器２の出力が一様であれば“０”または“１”が出る確率は１／２であるため、各々の数字がｋ回連続して出現する確率は（１／２）^{k} であり、例えば３０回連続して同じ数字が出現する確率は１／１０７３７４１８２４（すなわち、ほとんどゼロ）となるので、もし３０回連続して同じ数字が出現したら、この乱数発生器２は正常ではないと判断できるという考え方に基づくものである。

【００２８】すなわち、この１ビット乱数発生装置１は、図３に示すように、乱数発生器２、Ｄタイプフリップフロップなどのデータ保持器８、排他的論理和素子などの比較器９、カウンター１０および出力回路６から構成された検証データ出力型であり、乱数発生器２に同期信号が入力されると、乱数発生器２から乱数データとして「１」または「０」が出力される。このとき、乱数発生器２の入力信号および出力信号がデータ保持器８にも入力され、データ保持器８は、乱数発生器２から出力された前回の乱数データを保持して比較器９に出力する。また、比較器９には乱数発生器２の出力信号も入力され、比較器９は、乱数発生器２から出力された今回の乱数データとデータ保持器８に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号をカウンター１０に出力するとともに、両者が異なるときにはカウントクリア信号をカウンター１０に出力する。そして、カウンター１０には乱数発生器２の入力信号も入力され、カウンター１０はそのデータを出力回路６に出力し、出力回路６はそのデータを同一信号長の検証データとしてシリアルまたはパラレルに逐次出力する。

【００２９】したがって、この１ビット乱数発生装置１では、出力された同一信号長の検証データによって、乱数の一様性を検証するための統計処理が容易になる。

【００３０】図４は本発明に係る１ビット乱数発生装置の第４の実施形態を示す回路図である。

【００３１】この１ビット乱数発生装置１は、図４に示すように、乱数発生器２、Ｄタイプフリップフロップなどのデータ保持器８、排他的論理和素子などの第１の比較器１１、カウンター１０、レジスター１２、排他的論理和素子などの第２の比較器１３、制御回路１４および出力回路１５から構成された検証データ出力型であり、乱数発生器２に同期信号が入力されると、乱数発生器２から乱数データとして「１」または「０」が出力される。このとき、乱数発生器２の入力信号および出力信号がデータ保持器８にも入力され、データ保持器８は、乱数発生器２から出力された前回の乱数データを保持して第１の比較器１１に出力する。また、第１の比較器１１には乱数発生器２の出力信号も入力され、第１の比較器１１は、乱数発生器２から出力された今回の乱数データとデータ保持器８に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号をカウンター１０に出力するとともに、両者が異なるときにはカウントクリア信号をカウンター１０に出力する。そして、カウンター１０には乱数発生器２の入力信号も入力され、カウンター１０はそのデータを第２の比較器１３に出力し、第２の比較器１３は、レジスター１２のデータとカウンター１０の出力データとを比較し、前者より後者の方が大きいときにはデータ上書き信号を制御回路１４に出力するとともに、それ以外のときにはデータ保持信号を制御回路１４に出力する。制御回路１４は、データ上書き信号を受けたときにはカウンター１０の出力データをレジスター１２に書き込むとともに、データ保持信号を受けたときにはレジスター１２のデータを保持するように制御し、出力回路１５は、レジスター１２に保持されたデータを最長の同一信号長の検証データとしてシリアルまたはパラレルに逐次出力する。

【００３２】したがって、この１ビット乱数発生装置１では、出力された最長の同一信号長の検証データによって、乱数の一様性を検証するための統計処理が容易になる。

【００３３】図５は本発明に係る１ビット乱数発生装置の第５の実施形態を示す回路図である。

【００３４】この１ビット乱数発生装置２４は、図５に示すように、乱数発生器２、Ｄタイプフリップフロップなどのデータ保持器８、排他的論理和素子などの第１の比較器１１、カウンター１０、レジスター１２、排他的論理和素子などの第２の比較器１３、制御回路１４および排他的論理和素子などの第３の比較器１６から構成された検証信号出力型であり、乱数発生器２に同期信号が入力されると、乱数発生器２から乱数データとして「１」または「０」が出力される。このとき、乱数発生器２の入力信号および出力信号がデータ保持器８にも入力され、データ保持器８は、乱数発生器２から出力された前回の乱数データを保持して第１の比較器１１に出力する。また、第１の比較器１１には乱数発生器２の出力信号も入力され、第１の比較器１１は、乱数発生器２から出力された今回の乱数データとデータ保持器８に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号をカウンター１０に出力するとともに、両者が異なるときにはカウントクリア信号をカウンター１０に出力する。そして、カウンター１０には乱数発生器２の入力信号も入力され、カウンター１０はそのデータを第２の比較器１３に出力し、第２の比較器１３は、レジスター１２のデータとカウンター１０の出力データとを比較し、前者より後者の方が大きいときにはデータ上書き信号を制御回路１４に出力するとともに、それ以外のときにはデータ保持信号を制御回路１４に出力する。制御回路１４は、データ上書き信号を受けたときにはカウンター１０の出力データをレジスター１２に書き込むとともに、データ保持信号を受けたときにはレジスター１２のデータを保持するように制御し、第３の比較器１６は、レジスター１２に保持されたデータと予め設定された比較データとを比較して最長の同一信号長の検証信号を逐次出力する。

【００３５】したがって、この１ビット乱数発生装置２４では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

【００３６】図６は本発明に係る１ビット乱数発生装置の第６の実施形態を示す回路図である。

【００３７】この１ビット乱数発生装置１は、図６に示すように、乱数発生器２、Ｄタイプフリップフロップなどのデータ保持器８、排他的論理和素子などの比較器９、第１のカウンター１７、第２のカウンター１８、デコーダー１９、複数個（ｎ個）の第３のカウンター２０、複数個（ｎ個）のレジスター２１および制御回路２２から構成された検証データ出力型であり、乱数発生器２に同期信号が入力されると、乱数発生器２から乱数データとして「１」または「０」が出力される。このとき、第１のカウンター１７が計数する一定回数での各同一信号長（１～ｎ）の出現率をカウントし、第１のカウンター１７が計数する一定回数ごとにレジスター２１に書き込み、各同一信号長の分布を逐次出力する。

【００３８】すなわち、乱数発生器２の入力信号および出力信号がデータ保持器８にも入力され、データ保持器８は、乱数発生器２から出力された前回の乱数データを保持して比較器９に出力する。また、比較器９には乱数発生器２の出力信号も入力され、比較器９は、乱数発生器２から出力された今回の乱数データとデータ保持器８に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号を制御回路２２に出力するとともに、両者が異なるときにはカウントクリア信号を制御回路２２に出力する。一方、乱数発生器２の入力信号は第１のカウンター１７および制御回路２２にも入力され、第１のカウンター１７は一定回数を計数して制御回路２２に出力する。さらに、乱数発生器２の入力信号は第２のカウンター１８にも入力され、第２のカウンター１８は、比較器９からカウントアップ信号を受けたときにはカウントアップしてデコーダー１９に出力するとともに、比較器９からカウントクリア信号を受けたときにはカウントクリアしてデコーダー１９に出力する。これを受けてデコーダー１９は、第２のカウンター１８の出力データをデコードして各信号長ごとに第３の各カウンター２０へ出力し、各カウンター２０はこの出力データをカウントして各レジスター２１に出力する。そして、各レジスター２１は、制御回路２２による制御下で、比較器９の出力データと第１のカウンター１７で計数された一定回数ごとの信号とに基づいて同一信号長の検証データをシリアルまたはパラレルに逐次出力する。

【００３９】したがって、この１ビット乱数発生装置１では、出力された各カウント数（検証データ）によって、乱数の一様性を検証するための統計処理が容易になる。

【００４０】図７は本発明に係る１ビット乱数発生装置の第７の実施形態を示す回路図である。

【００４１】この１ビット乱数発生装置１は、図７に示すように、乱数発生器２、Ｄタイプフリップフロップなどのデータ保持器８、排他的論理和素子などの比較器９、第１のカウンター１７、第２のカウンター１８、デコーダー１９、複数個（ｎ個）の第３のカウンター２０、複数個（ｎ個）のレジスター２１、制御回路２２および選択回路２３から構成された検証データ出力型であり、乱数発生器２に同期信号が入力されると、乱数発生器２から乱数データとして「１」または「０」が出力される。このとき、第１のカウンター１７が計数する一定回数での各同一信号長（１～ｎ）の出現率をカウントし、第１のカウンター１７が計数する一定回数ごとにレジスター２１に書き込み、各同一信号長の分布を外部からの選択データで選択できる選択回路２３にて逐次出力する。

【0042】すなわち、乱数発生器2の入力信号および出力信号がデータ保持器8にも入力され、データ保持器8は、乱数発生器2から出力された前回の乱数データを保持して比較器9に出力する。また、比較器9には乱数発生器2の出力信号も入力され、比較器9は、乱数発生器2から出力された今回の乱数データとデータ保持器8に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号を制御回路22に出力するとともに、両者が異なるときにはカウントクリア信号を制御回路22に出力する。一方、乱数発生器2の入力信号は第1のカウンター17および制御回路22にも入力され、第1のカウンター17は一定回数を計数して制御回路22に出力する。さらに、乱数発生器2の入力信号は第2のカウンター18にも入力され、第2のカウンター18は、比較器9からカウントアップ信号を受けたときにはカウントアップしてデコーダー19に出力するとともに、比較器9からカウントクリア信号を受けたときにはカウントクリアしてデコーダー19に出力する。これを受けてデコーダー19は、第2のカウンター18の出力データをデコードして各信号長ごとに第3の各カウンター20へ出力し、各カウンター20はこの出力データをカウントして各レジスター21に出力する。そして、各レジスター21は、制御回路22による制御下で、比較器9の出力データと第1のカウンター17で計数された一定回数ごとの信号とに基づいて同一信号長の検証データを選択回路23にシリアルまたはパラレルに逐次出力する。さらに、選択回路23に外部から選択データが入力されると、選択回路23はレジスター21の出力データをその選択データに基づいて適宜選択して出力する。

【0043】したがって、この1ビット乱数発生装置1では、出力された同一信号長の分布データによって、乱数の一様性を検証するための統計処理が容易になる。

【0044】図8は本発明に係る多数ビット乱数発生装置の第1の実施形態を示す回路図である。

【0045】この多数ビット乱数発生装置25は、図8に示すように、上述した検証データ出力型の1ビット乱数発生装置1を複数個（n個）並列に接続し、これに選択回路26を付設したものであり、選択回路26に外部から選択データが入力されると、選択回路26は、1ビット乱数発生装置1から出力された検証データをその選択データに基づいてビットごとに選択して出力する。

【0046】したがって、この多数ビット乱数発生装置25では、出力された一様性検証データによって、乱数の一様性を検証するための統計処理が容易になる。

【0047】図9は本発明に係る多数ビット乱数発生装置の第2の実施形態を示す回路図である。

【0048】この多数ビット乱数発生装置25は、図9に示すように、上述した検証信号出力型の1ビット乱数発生装置24を複数個（n個）並列に接続し、これに選択回路27を付設したものであり、選択回路27に外部から選択データが入力されると、選択回路27は、1ビット乱数発生装置24から出力された検証信号をその選択データに基づいてビットごとに選択して出力する。

【0049】したがって、この多数ビット乱数発生装置25では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

【0050】図10は本発明に係る確率発生装置の第1の実施形態を示す回路図である。

【0051】この確率発生装置30は、図10に示すように、上述した検証データ出力型の1ビット乱数発生装置1、シフトレジスター31、カウンター32、レジスター33および比較器34から構成されており、1ビット乱数発生装置1からから出力された乱数データはシフトレジスター31に入力され、シフトレジスター31はこの乱数データをシリアルデータからパラレルデータへ変換してレジスター33に出力する。一方、1ビット乱数発生装置1の入力信号はカウンター32にも入力され、カウンター32は一定のパラレルデータのビット長を計数してレジスター33に出力する。すると、レジスター33は、カウンター32で計数された周期ごとにシフトレジスター31のパラレルデータを保持する。そして、比較器34は、レジスター33に保持されたデータと予め設定された確率上限データおよび確率下限データとを比較し、レジスター33内のデータが確率上限データと確率下限データとの間にある場合には“当たり”、それ以外の場合には“外れ”の確率信号を出力する。

【0052】したがって、この確率発生装置30では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を検証することが容易であることから、確率の信頼性を評価することも容易になる。

【0053】図11は本発明に係る確率発生装置の第2の実施形態を示す回路図である。

【0054】この確率発生装置30は、図11に示すように、上述した検証信号出力型の1ビット乱数発生装置24、シフトレジスター31、カウンター32、レジスター33および比較器34から構成されており、1ビット乱数発生装置24から出力された乱数データはシフトレジスター31に入力され、シフトレジスター31はこの乱数データをシリアルデータからパラレルデータへ変換してレジスター33に出力する。一方、1ビット乱数発生装置24の入力信号はカウンター32にも入力され、カウンター32は一定のパラレルデータのビット長を計数してレジスター33に出力する。すると、レジスター33は、カウンター32で計数された周期ごとにシフトレジスター31のパラレルデータを保持する。そして、比較器34は、レジスター33に保持されたデータと予め設定された確率上限データおよび確率下限データとを比較し、レジスター33内のデータが確率上限デー

タと確率下限データとの間にある場合には“当たり”、それ以外の場合には“外れ”の確率信号を出力する。

【００５５】したがって、この確率発生装置３０では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を検証することが容易であることから、確率の信頼性を評価することも容易になる。

【００５６】図１２は本発明に係る確率発生装置の第３の実施形態を示す回路図、図１３は本発明に係る確率発生装置の第４の実施形態を示す回路図である。

【００５７】これらの確率発生装置３０は、図１２および図１３に示すように、上述した多数ビット乱数発生装置２５および比較器３５から構成されており、多数ビット乱数発生装置２５から出力された乱数データ（パラレルデータ）は比較器３５に入力され、比較器３５は、この乱数データと予め設定された確率上限データおよび確率下限データとを比較し、乱数データが確率上限データと確率下限データとの間にある場合には“当たり”、それ以外の場合には“外れ”の確率信号を出力する。

【００５８】したがって、この確率発生装置３０では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を検証することが容易であることから、確率の信頼性を評価することも容易になる。

【００５９】

【発明の効果】以上説明したように、本発明のうち請求項１～７に係る発明によれば、乱数データの出現一様性を自ら検証することができ、使用者が統計処理を行う必要がなくなることから、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な１ビット乱数発生装置を提供することができる。

【００６０】また、本発明のうち請求項８、９に係る発明によれば、乱数データの出現一様性を自ら検証することができ、使用者が統計処理を行う必要がなくなることから、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な多数ビット乱数発生装置を提供することができる。

【００６１】さらに、本発明のうち請求項１０、１１に係る発明によれば、乱数データの出現一様性を自ら検証することができ、使用者が統計処理を行う必要がなくなることから、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な確率発生装置を提供することができる。

【図面の簡単な説明】

【図１】本発明に係る１ビット乱数発生装置の第１の実施形態を示す回路図である。

【図２】本発明に係る１ビット乱数発生装置の第２の実施形態を示す回路図である。

【図３】本発明に係る１ビット乱数発生装置の第３の実施形態を示す回路図である。

【図４】本発明に係る１ビット乱数発生装置の第４の実施形態を示す回路図である。

【図５】本発明に係る１ビット乱数発生装置の第５の実施形態を示す回路図である。

【図６】本発明に係る１ビット乱数発生装置の第６の実施形態を示す回路図である。

【図７】本発明に係る１ビット乱数発生装置の第７の実施形態を示す回路図である。

【図８】本発明に係る多数ビット乱数発生装置の第１の実施形態を示す回路図である。

【図９】本発明に係る多数ビット乱数発生装置の第２の実施形態を示す回路図である。

【図１０】本発明に係る確率発生装置の第１の実施形態を示す回路図である。

【図１１】本発明に係る確率発生装置の第２の実施形態を示す回路図である。

【図１２】本発明に係る確率発生装置の第３の実施形態を示す回路図である。

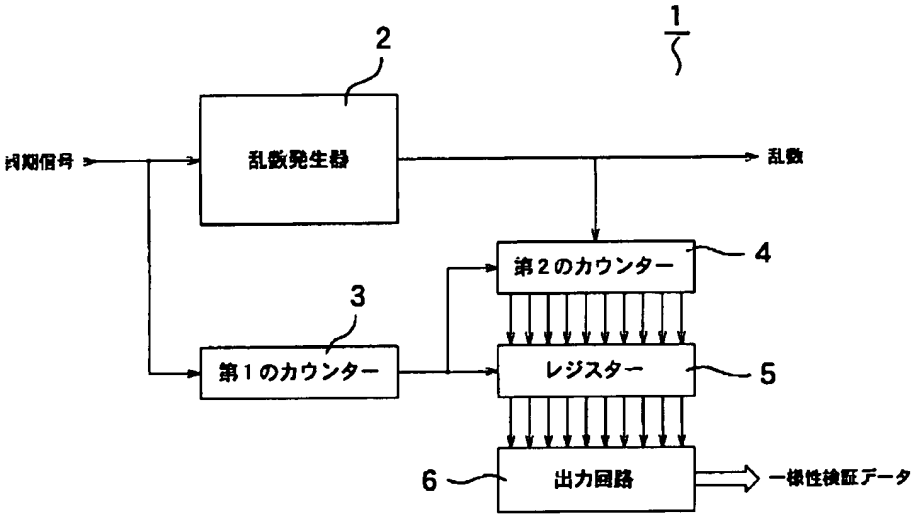
【図１３】本発明に係る確率発生装置の第４の実施形態を示す回路図である。

【符号の説明】

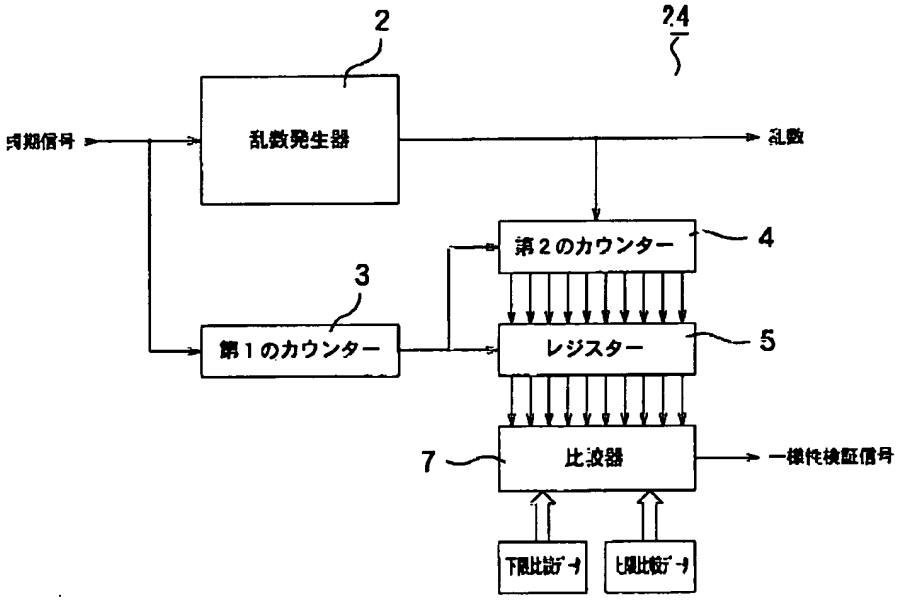
１……１ビット乱数発生装置
２……乱数発生器
３……第１のカウンター
４……第２のカウンター
５……レジスター
６……出力回路
７……比較器
８……データ保持器
９……比較器
１０……カウンター
１１……第１の比較器
１２……レジスター
１３……第２の比較器
１４……制御回路
１５……出力回路
１６……第３の比較器
１７……第１のカウンター
１８……第２のカウンター
１９……デコーダー
２０……第３のカウンター
２１……レジスター
２２……制御回路
２３……選択回路
２４……１ビット乱数発生装置
２５……多数ビット乱数発生装置
２６……選択回路
２７……選択回路
３０……確率発生装置
３１……シフトレジスター
３２……カウンター
３３……レジスター

34……比較器　　35……比較器

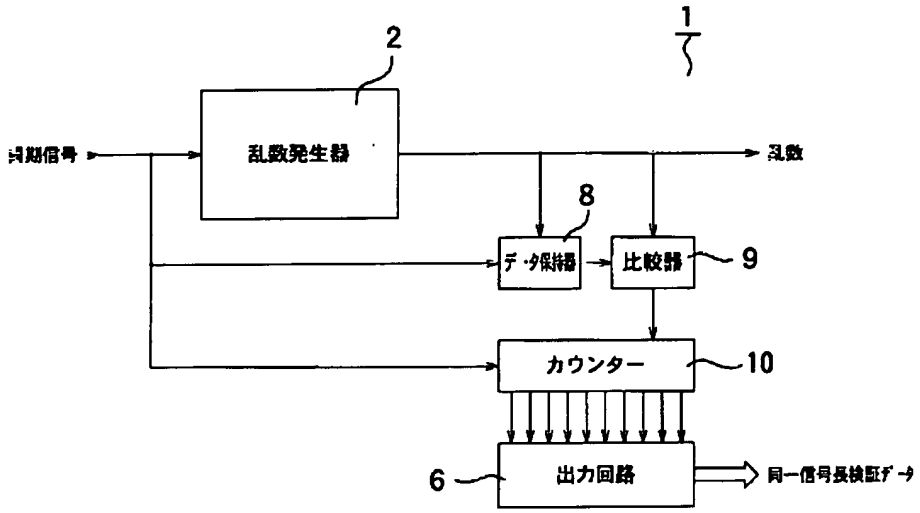
【図1】



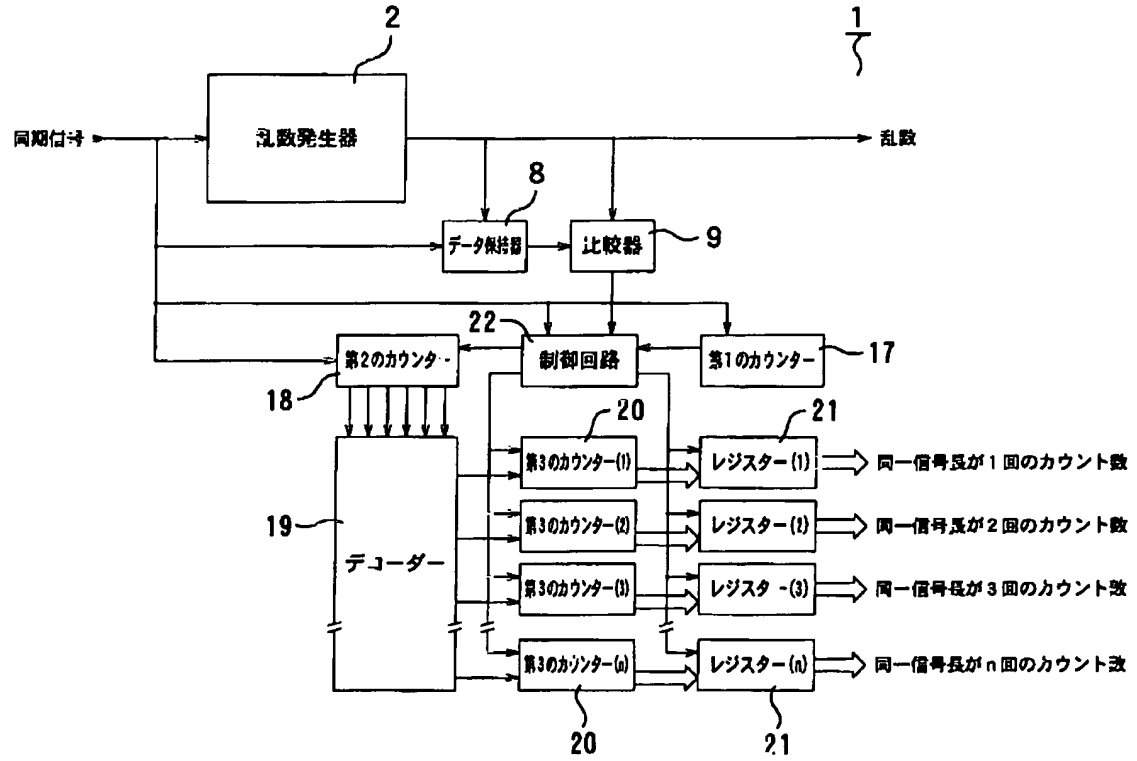
【図2】



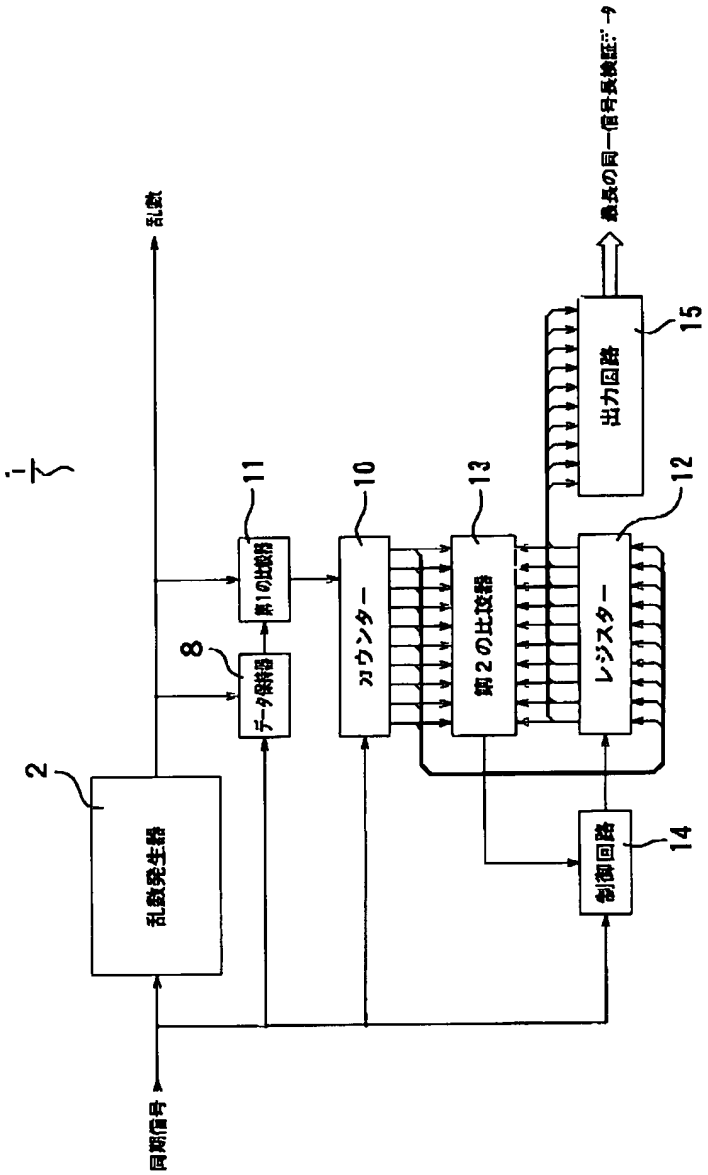
【図3】


1
2
乱数発生器
乱数
8
データ保持器
比較器
9
カウンター
10
6
出力回路
同一信号長検証データ

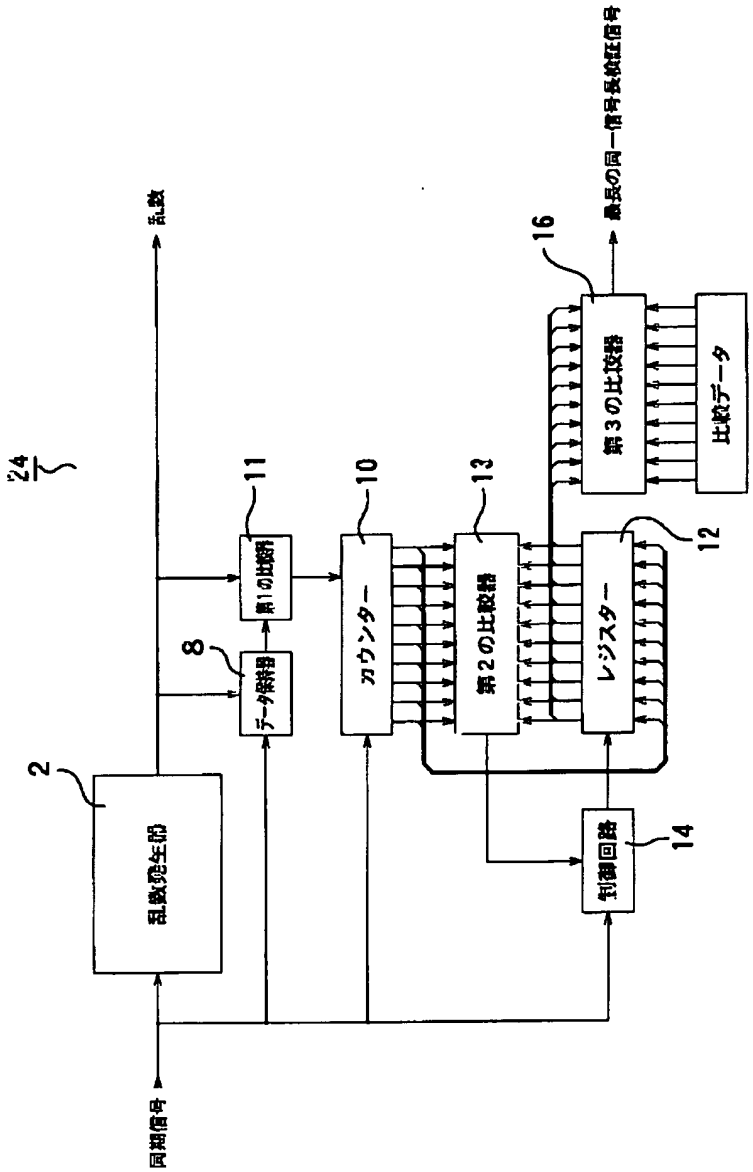
【図6】


1
2
乱数発生器
乱数
8
データ保持器
比較器
9
22
制御回路
第2のカウンター
第1のカウンター
17
18
20
21
19
デコーダー
第3のカウンター(1)
第3のカウンター(2)
第3のカウンター(3)
第3のカウンター(n)
レジスター(1)
レジスター(2)
レジスター(3)
レジスター(n)
同一信号長が1回のカウント数
同一信号長が2回のカウント数
同一信号長が3回のカウント数
同一信号長がn回のカウント数

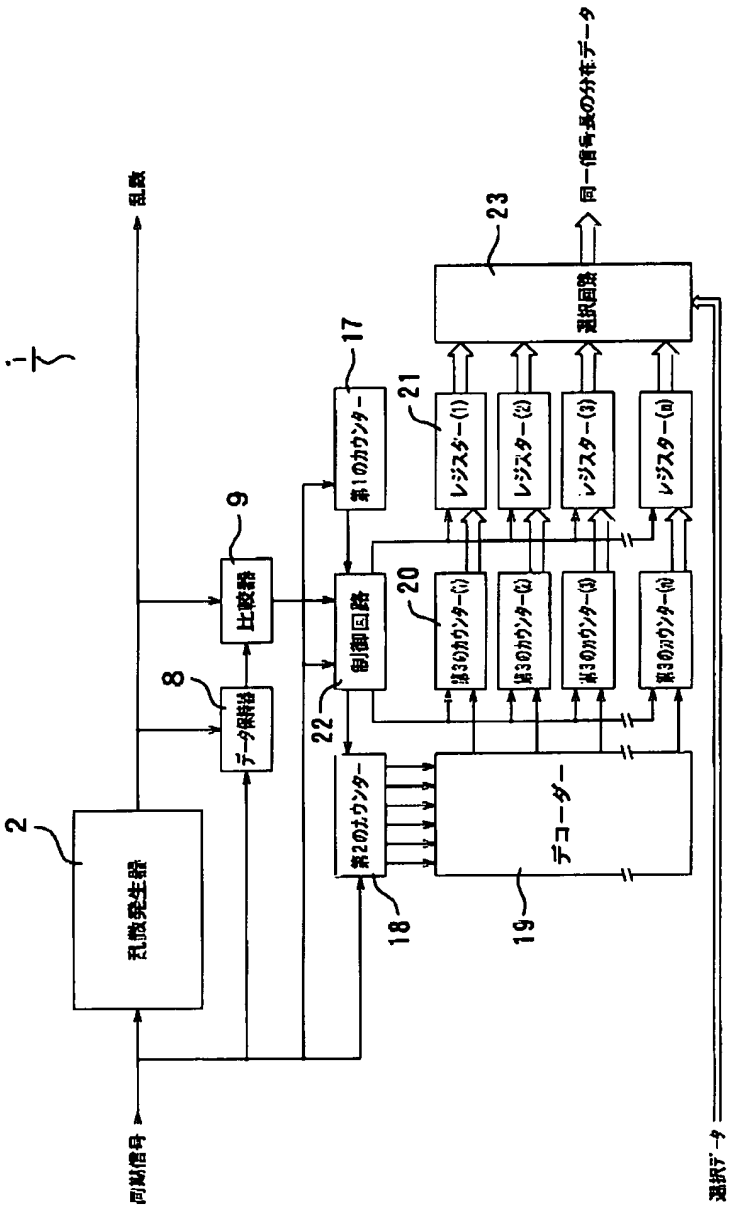
【図4】


1
乱数
最長の同一信号長検証データ
出力回路
15
11
10
13
12
第1の比較器
カウンター
第2の比較器
レジスター
8
データ保持器
2
乱数発生器
制御回路
14
同期信号

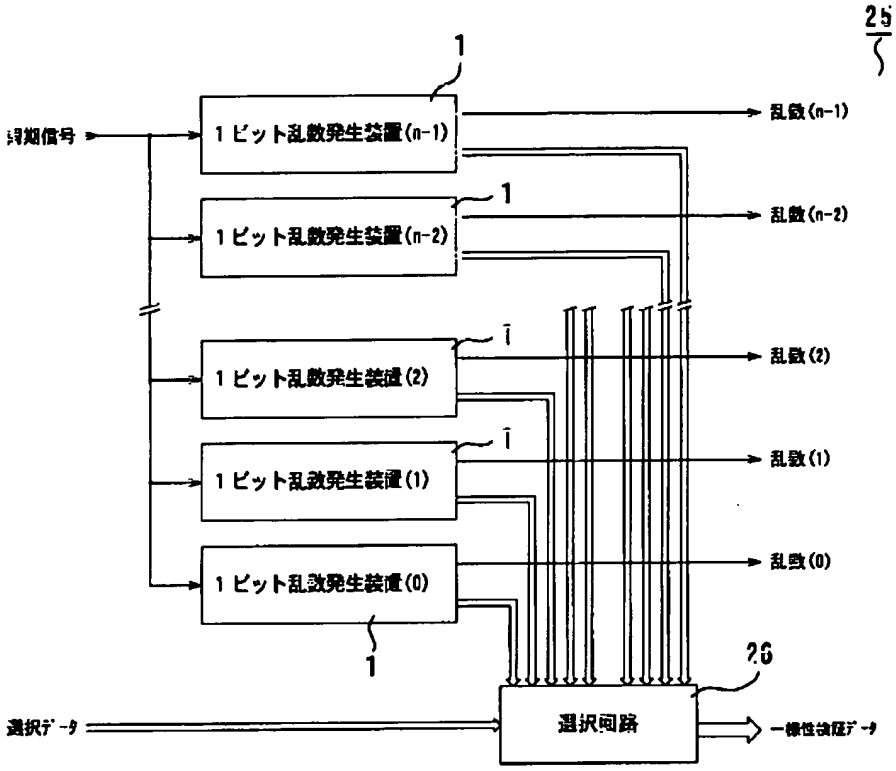
【図5】


24
乱数
最長の同一信号長検証信号
16
第3の比較器
比較データ
11
第1の比較器
10
カウンター
13
第2の比較器
12
レジスター
8
データ保持器
2
乱数発生部
制御回路
14
同期信号

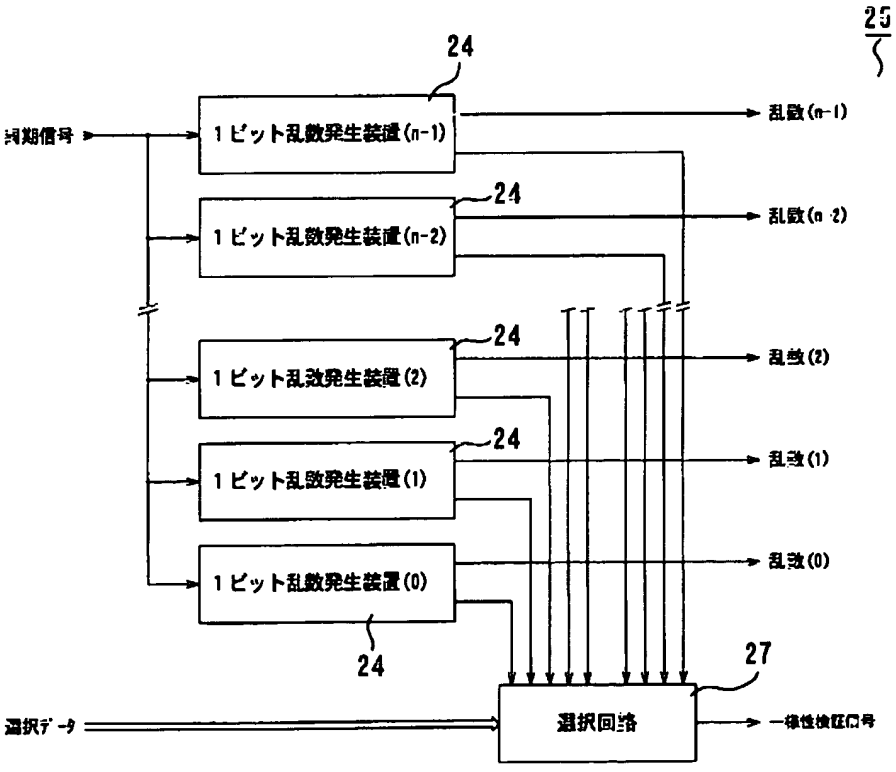
【図7】


1
乱数
同一信号長の分布データ
23
選択回路
17
第1のカウンター
21
レジスター(1)
レジスター(2)
レジスター(3)
レジスター(n)
9
比較器
8
データ保持器
20
制御回路
第3のカウンター(1)
第3のカウンター(2)
第3のカウンター(3)
第3のカウンター(n)
22
第2のカウンター
デコーダー
2
乱数発生器
18
19
同期信号
選択データ

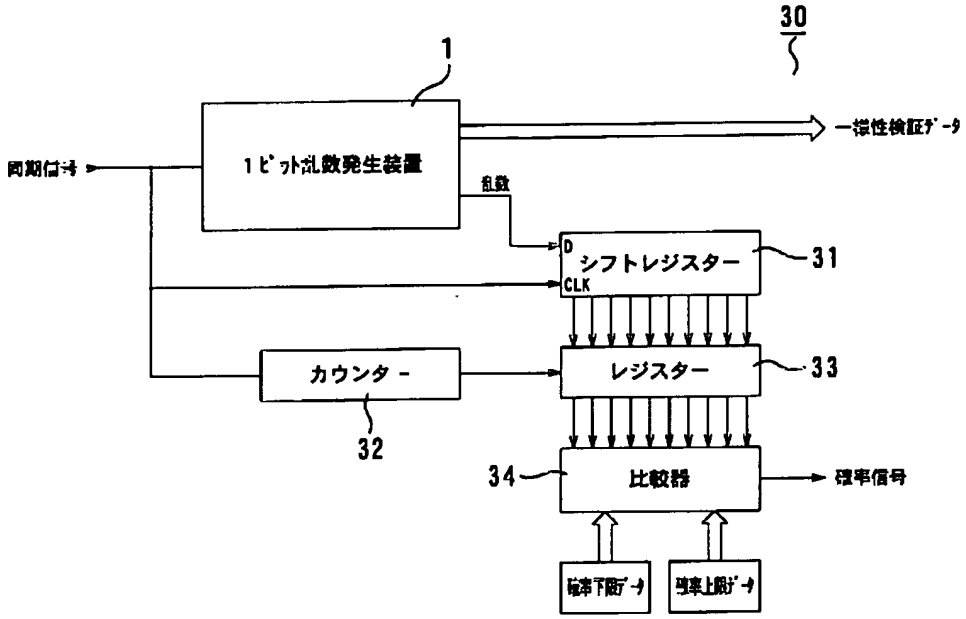
【図8】


25
1
同期信号
1ビット乱数発生装置(n-1)
乱数(n-1)
1
1ビット乱数発生装置(n-2)
乱数(n-2)
1
1ビット乱数発生装置(2)
乱数(2)
1
1ビット乱数発生装置(1)
乱数(1)
1ビット乱数発生装置(0)
乱数(0)
1
26
選択データ
選択回路
一様性検証データ

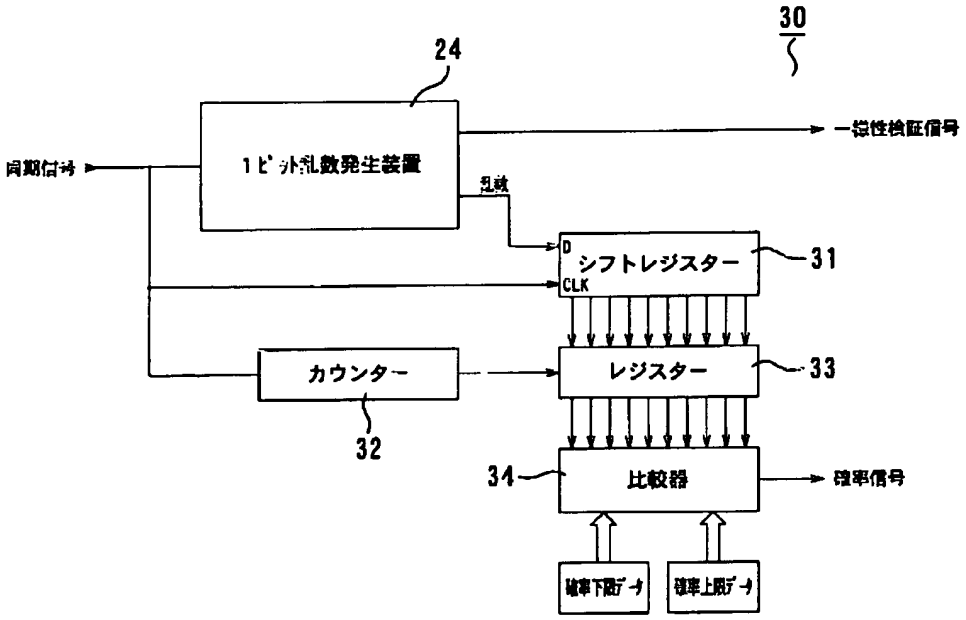
【図9】


25
24
同期信号
1ビット乱数発生装置(n-1)
乱数(n-1)
24
1ビット乱数発生装置(n-2)
乱数(n-2)
24
1ビット乱数発生装置(2)
乱数(2)
24
1ビット乱数発生装置(1)
乱数(1)
1ビット乱数発生装置(0)
乱数(0)
24
27
選択データ
選択回路
一様性検証信号

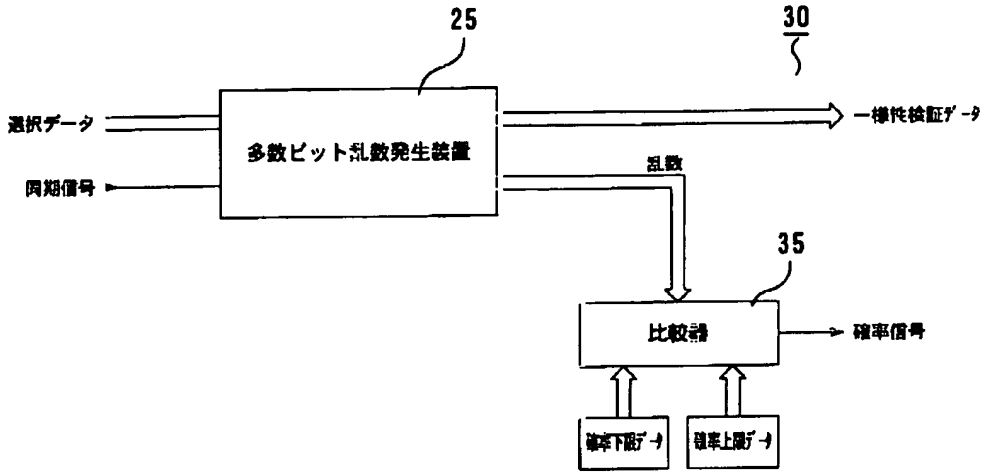
【図10】


30
1
1ビット乱数発生装置
同期信号
一様性検証データ
乱数
D
CLK
シフトレジスター
31
カウンター
32
レジスター
33
34
比較器
確率信号
確率下限データ
確率上限データ

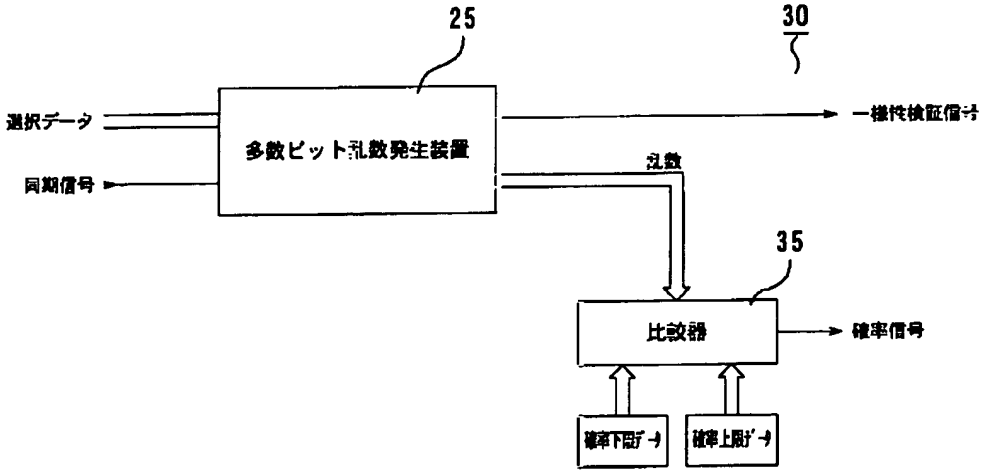
【図11】


30
24
1ビット乱数発生装置
同期信号
一様性検証信号
乱数
D
CLK
シフトレジスター
31
カウンター
32
レジスター
33
34
比較器
確率信号
確率下限データ
確率上限データ

【図12】



【図13】



フロントページの続き

(72)発明者　清水　隆邦
東京都港区新橋５丁目36番11号　いわき電子株式会社内

(72)発明者　鯉渕　美佐子
東京都港区新橋５丁目36番11号　いわき電子株式会社内

Ｆターム(参考)　5J104 FA00 GA00